CLAIMS

I claim:

1. A method of authenticating a computing device on a Wi-Fi communications network comprising the steps of:

   obtaining an access point identifier at a computing device, wherein said access point identifier identifies an access point of a Wi-Fi communications network;

   selecting, at said computing device, a set of authentication parameters associated with said access point identifier; and

   implementing an authentication process employing said set of authentication parameters.

2. The method of claim 1, wherein said access point identifier is a basic service set identifier (BSSID).

3. The method of claim 2, wherein said step of obtaining an access point identifier, comprises the step of

   receiving said basic service set identifier from said access point.

4. The method of claim 1, wherein said set of authentication parameters are pre-stored in a tamper-resistant physical token..

5. The method of claim 4, further comprising the step of

   installing said tamper-resistant physical token at said computing device.

6. The method of claim 5, wherein said tamper-resistant physical token is adapted to be inserted into a communications port at said computing device.

7. The method of claim 4, wherein said tamper-resistant physical token further comprises

   one or more additional sets of authentication parameters, wherein each set of authentication parameters is associated with a unique access point identifier.

8. The method of claim 7, wherein each of said unique access point identifiers is stored in said tamper-resistant physical token and in relation to its associated set of authentication parameters.

9. The method of claim 1, further comprising the step of

   permitting said computing device to access said Wi-Fi communications network via said access point if said authentication process results in a successful authentication of said computing device.

10. The method of claim 5, wherein said set of authentication parameters comprises a first secret cryptographic key.

11. The method of claim 10, wherein said authentication process comprises the steps of:

transmitting a first challenge, wherein said first challenge comprises an encrypted first random number and a unique identifier associated with said computing device, said encrypted first random number being encrypted with said first secret cryptographic key; and

receiving a second challenge, wherein said second challenge comprises an encrypted second random number, said second random number generated at said access point and encrypted with said a secret cryptographic key stored at said access point and associated with said unique identifier.

12. The method of claim 11, wherein said unique identifier is a serial number of said tamper-resistant physical token.

13. The method of claim 11, wherein said set of authentication parameters further comprises:

a network receive cryptographic key, and

a network send cryptographic key.

14. The method of claim 13, further comprising the steps of:

encrypting said first challenge with said network send cryptographic key; and

decrypting said second challenge with said network receive cryptographic key.

15. A communications system comprising:

one or more authentication devices,

one or more client devices, wherein each client device includes a unique tamper-resistant physical token comprising:

one or more unique sets of authentication parameters, wherein each set of authentication parameters is associated with one or more of said one or more authentication devices;

a random number generator; and

a unique serial number.

16. The system of claim 15, wherein each client device further includes a wireless communications transceiver to communicate with one of said one or more authentication device via a wireless channel.

17. The system of claim 16, wherein said wireless channel is an IEEE 802.11 wireless channel.

18. The system of claim 15, wherein one or more authentication devices are Wi-Fi access points.
19. The system of claim 18, wherein at least two Wi-Fi access points are associated with different Wi-Fi networks.
20. The system of claim 19, wherein each of said one or more unique sets of authentication parameters is associated with an access point identifier.
21. The system of claim 20, wherein said access point identifier is a basic service set identifier (BSSID).
22. The system of claim 15, wherein each tamper-resistant physical token is adapted to be installed via a communications port at said computing device.